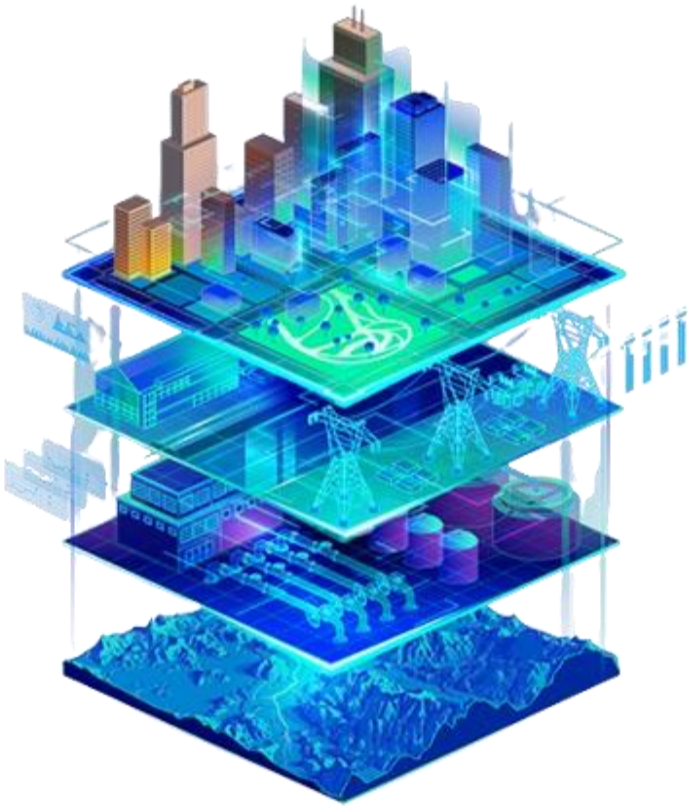

LIVRABLE 2

Sécurité du S.I.

Groupe 3

1 Table des matières

2 Table des images

3 Présentation de l’équipe d’ESN Numerica

- Mathéo Penteado
- Théo Journée
- Erwan Hertz
- Thomas Loridan
- Martin Wroblewski

4 Introduction

4.1 Contexte

Le groupe **ASSURANCESPLUS**, spécialisé dans les services d'assurance, a été victime d'une attaque par rançongiciel, paralysant totalement les activités de l'une de ses agences. Ce sinistre a mis en lumière des failles importantes dans la sécurisation des systèmes d'information des agences. En réponse à cette crise, le groupe a mandaté l'**ESN Numerica** pour rétablir le fonctionnement de l'agence touchée et surtout pour prévenir de futurs incidents de cette ampleur.

4.2 Problématique

Comment assurer une unification, une sécurisation optimale et une résilience renforcée des systèmes d'information d'**ASSURANCESPLUS** tout en répondant aux besoins spécifiques des agences actuelles et des futures agences, dans un contexte de croissance et d'évolution des menaces cybernétiques

5 Questionnaire de sécurité

5.1 Affiche de sensibilisation

Dans le cadre de la refonte de l'architecture SI de nos agences, nous avons réalisé une affiche destinée aux employées afin de les sensibiliser à la sécurité informatique.

Celle-ci retrace différents danger et axes de sécurité à appliquer afin d'éviter les risques.

Figure 1 : Affiche de sensibilisation.

5.2 Questionnaire de sensibilisation

Un questionnaire destiné aux responsables informatiques a été réalisé. L'objectif de celui-ci est d'identifier le type d'infrastructure déjà en place au sein de l'agence mais aussi de relever les axes de progressions.

Le lien / QRCode de ce formulaire est disponible ci-dessous :

https://urls.fr/RLQ_72

Figure 2 : QR Code, du formulaire.

Les réponses à ce formulaire sont fournies dans le document du lien suivant :
https://drive.google.com/file/d/1Zdj_LBilGN96Vfw7d0STYIQT1QPjgRkx/view?usp=drive_link

Ce lien est disponible dans le message de remerciement du formulaire.

(Cette méthode n'est pas professionnelle, cependant les commentaires disponibles dans ce système de formulaire ne fonctionnent pas).

7 Politique de filtrage

la Politique de Filtrage Firewall pour ASSURANCESPLUS.

Ordre	Section	Source	Destination	Port/Protocole	Action	Description
1	Règles d'autorisation vers le pare-feu	Serveurs Admin (192.168.80.1)	Interface Admin Pare-feu	22 (SSH)	Autoriser	Accès SSH pour gestion
2	Règles d'autorisation vers le pare-feu	Serveurs Supervision (192.168.81.1/24)	Interface Supervision Pare-feu	161 (SNMPv3)	Autoriser	Supervision via SNMP version 3
3	Règles d'autorisation vers le pare-feu	Pare-feu	Serveur NTP (pool.ntp.org)	123 (UDP/NTP)	Autoriser	Synchronisation horaire sécurisée avec le serveur NTP.
4	Règles d'autorisation émises par le pare-feu	Pare-feu	Serveur Logs Centralisé (192.168.1	514 (Syslog)	Autoriser	Envoi des journaux vers le serveur de logs centralisé.
5	Règles d'autorisation émises par le pare-feu	Pare-feu	Serveur Logs Centralisé	514 (Syslog)	Autoriser	Envoi des journaux
6	Règles de protection du pare-feu	Toutes	Pare-feu	Tous	Bloquer (DROP/REJECT	Bloquer tout trafic non autorisé et journaliser
7	Règles métiers internes	Siège (192.168.80.0/24)	Agences (ERP)	5432 (PostgreSQL)	Autoriser	Communication ERP entre siège et agences
8	Règles métiers internes	Interne	Office 365	443 (HTTPS)	Autoriser	Accès à Office 365
9	Règles métiers externes	Proxy Interne	Internet	80, 443 (HTTP/HTTPS)	Autoriser	Navigation via proxy sécurisé, avec filtrage de contenu
10	Règles antiparasites	Toutes	Toutes	137, 138, 445 (UDP/TCP)	Bloquer	Bloquer les communications NetBIOS inutiles
11	Règles antiparasites	Toutes	Toutes	ICMP (ping)	Bloquer	Bloquer les pings non nécessaires
12	Règles spécifiques	Interne	DMZ	443, 80 (http/https)	Autoriser	Autoriser les accès des services internes vers la DMZ pour certaines applications
13	Règle d'interdiction finale	Toutes	Toutes	Tous	Bloquer	Blocage global par défaut
14	Règle de mise à jour	interne	Serveurs de mise à jour	80, 443 (HTTP/HTTPS)	Autoriser	Accès aux serveurs de mise à jour (Windows/Linux)
15	Règles métiers internes	net_direction	Serveur de gestion des sinistres	443 (HTTPS)	Autoriser	Permettre à la direction d'accéder aux outils de gestion des sinistres.
16	Règles métiers internes	net_juridique	Serveur clients	443 (HTTPS)	Autoriser	Autoriser le service juridique à consulter les dossiers client pour des besoins de conformité légale.
17	Règles métiers internes	net_commercial	Serveur conseil commerce	443 (HTTPS)	Autoriser	Donner aux commerciaux l'accès aux outils de gestion commerciale.
18	Règles spécifiques	net_admin, net_operateurs	serveur cybersécurité	443 (HTTPS)	Autoriser	Permettre aux administrateurs et opérateurs d'accéder aux dossiers sensibles pour des opérations spécifiques.
19	Règles spécifiques	Toutes sauf net_admin, net_operateurs	serveur cybersécurité	443 (HTTPS)	Bloquer	Bloquer tout accès non autorisé aux données sensibles.
20	Règles de gestion des rôles	net_admin, net_keyuser	serveur roles	443 (HTTPS)	Autoriser	Permettre aux administrateurs et KeyUsers de superviser et gérer les rôles inférieurs.
21	Règles d'interdiction antiparasites	Rôles non pertinents	Services non autorisés	Tous	Bloquer	Bloquer les accès des rôles vers des services ou flux non pertinents (ex. commerciaux accédant aux ressources des sinistres).
22	Règles métiers internes	net_agences	serveur ERP	5432 (PostgreSQL)	Autoriser	Permettre aux agences d'accéder au système ERP (complément à la règle 5).
23	Règles spécifiques	net_clients	Serveurs de mise à jour	80, 443 (HTTP/HTTPS)	Autoriser	Permettre aux clients des sinistres ou outils commerciaux de télécharger les mises à jour logicielles nécessaires.

Figure 3 : Tableau politique de filtrage.

- La politique de filtrage firewall d'ASSURANCESPLUS vise à sécuriser les flux de communication au sein du système d'information tout en permettant une gestion efficace des accès nécessaires. Elle est structurée autour de règles précises, qui équilibrent protection et fonctionnalité, en appliquant un principe de moindre privilège.

Détail de la politique de Filtrage Réseau pour ASSURANCESPLUS

Cette politique est fondée sur un modèle de **sécurité.** Elle est structurée en **6 sections** :

Ordre	Contenu
Section n°1	Règles d'autorisation des flux à destination du pare-feu
Section n°2	Règles de protection du pare-feu
Section n°3	Règles d'autorisation des flux métiers
Section n°4	Règles d'autorisation des flux émis par le pare-feu
Section n°5	Règles "antiparasites"
Section n°6	Règle d'interdiction finale

1. **Règles d'autorisation des flux à destination du pare-feu**

   (Ligne 1) - SSH pour gestion :

   Permet uniquement aux serveurs administratifs (192.168.80.1) d'accéder au pare-feu via le port 22 (SSH).

   But : Garantir un accès sécurisé au pare-feu pour les opérations d'administration.

   (Ligne 2) - Supervision SNMPv3 :

   Autorise la supervision sécurisée du pare-feu depuis les serveurs de supervision internes (192.168.81.1/24) via le protocole SNMP version 3 (port 161).

   But : Faciliter la surveillance et le suivi de l'état du pare-feu par des outils de supervision dédiés.

   (Ligne 3) - Synchronisation NTP :

   Permet au pare-feu de synchroniser son horloge avec le serveur NTP public (pool.ntp.org) via le port UDP 123.

   But : Assurer une synchronisation horaire précise, essentielle pour les journaux et les communications réseau.

2. **Règles de protection du pare-feu**

   (Ligne 6) - Blocage des flux non autorisés :

   Bloque tout trafic non explicitement autorisé et journalise les tentatives d'accès.

   But : Renforcer la politique de moindre privilège et protéger le pare-feu contre des accès non autorisés.

3. **Règles de flux métiers**

a. Métiers internes

(Ligne 7) - Communication ERP :

Permet la communication entre le siège (192.168.80.0/24) et les agences via le système ERP (port 5432 pour PostgreSQL).

But : Faciliter les opérations métiers quotidiennes nécessitant un accès au système ERP.

(Ligne 8) - Accès à Office 365 :

Autorise les utilisateurs internes à accéder aux outils Office 365 via le port HTTPS (443).

But : Assurer la collaboration interne via des outils bureautiques modernes.

(Ligne 15) - Direction vers gestion des sinistres :

Permet à la direction d'accéder aux outils de gestion des sinistres sur le serveur dédié via le port HTTPS (443).

But : Superviser les sinistres et prendre des décisions stratégiques.

(Ligne 16) - Juridique vers clients :

Permet au service juridique d'accéder aux données clients via le port HTTPS (443).

But : Vérifier la conformité et résoudre des litiges en lien avec les dossiers clients.

(Ligne 17) - Commercial vers gestion commerciale :

Donne accès aux commerciaux aux outils de gestion commerciale via le port HTTPS (443).

But : Gérer les relations clients et contrats de manière efficace.

(Ligne 18) - Admin/Opérateurs vers cybersécurité :
Autorise les administrateurs et opérateurs à accéder au serveur de cybersécurité pour des opérations sensibles via HTTPS (443).
But : Faciliter la gestion et l'investigation des incidents de sécurité.

(Ligne 20) - Gestion des rôles :
Permet aux administrateurs et KeyUsers de superviser et gérer les rôles inférieurs via le serveur dédié sur le port HTTPS (443).
But : Maintenir une gestion contrôlée des autorisations.

(Ligne 22) - Agences vers ERP :

Permet aux agences d'accéder au système ERP sur le port 5432 (PostgreSQL).

But : Synchroniser les données locales avec le siège pour des processus métiers optimisés.

(Ligne 23) - Mises à jour pour clients :
Autorise les clients à télécharger les mises à jour logicielles nécessaires via HTTP (80) et

HTTPS (443).
But : Maintenir les systèmes des clients à jour pour réduire les vulnérabilités.

b. Règles métiers externes

(Ligne 9) - Navigation via proxy :

Autorise la navigation web via le proxy interne pour accéder à Internet sur les ports HTTP (80) et HTTPS (443).

But : Contrôler l'accès au web, avec filtrage de contenu pour éviter les risques liés à des sites malveillants.

4. Règles d'autorisation des flux émis par le pare-feu

Ces règles concernent les flux sortants nécessaires au bon fonctionnement et au suivi du pare-feu.

(Ligne 4) - Envoi des journaux :
Autorise l'envoi des journaux du pare-feu vers le serveur de logs centralisé (192.168.10.20) via Syslog (port 514).
But : Centraliser les journaux pour l'audit et l'analyse des incidents.

5. Règles antiparasites

(Ligne 10) - Blocage NetBIOS :

Bloque les communications NetBIOS inutiles (ports 137, 138, 445) pour tous les flux.

But : Réduire les risques de propagation de menaces sur le réseau interne.

(Ligne 11) - Blocage ICMP :

Empêche les pings non nécessaires pour réduire les risques de reconnaissance réseau.

But : Limiter les tentatives de collecte d'informations sur le réseau.

(Ligne 21) - Blocage des accès non pertinents :

Interdit les flux entre des rôles ou services non pertinents (ex. commerciaux accédant à la gestion des sinistres).

But : Renforcer la segmentation réseau et éviter les abus.

6. **Règle d’interdiction finale**

   (Ligne 13) - Blocage global par défaut :

   Bloque tout flux non explicitement autorisé par une règle précédente.

   But : Implémenter une politique de moindre privilège pour sécuriser le réseau.

8 Scripts

8.1 Script déploiement d'un AD :

```
<#
.SYNOPSIS
Déploiement complet et sécurisé d'un environnement Active Directory.
.DESCRIPTION
Ce script déploie une forêt, un domaine, des OUs, des Groupes des utilisateurs, des GPOs, configure DNS.
implémente MFA et redondance, et sécurise les mots de passe.
.AUTHOR
Votre Nom
.LASTEDIT
02/12/2024
#>
# Attention de bien configurer l'IP, DNS etc au préalable


# Étape 1 : Définir les variables globales
$DomainName = "mon-domaine.local"
$NetBIOSName = "MONDOMAINE"
$ForestMode = "WinThreshold" # Niveau de forêt (Windows Server 2016+)
$OUBase = "OU=Utilisateurs,DC=mon-domaine,DC=local"
# Demander un mot de passe sécurisé pour le mode restauration AD DS et les utilisateurs
Write-Host "Veuillez entrer un mot de passe sécurisé pour le mode restauration AD DS :"
$SafeModePassword = Read-Host -AsSecureString
Write-Host "Veuillez entrer un mot de passe par défaut pour les utilisateurs créés :"
$UserPassword = Read-Host -AsSecureString


# Étape 2 : Installation des rôles nécessaires
Write-Host "Installation des rôles Active Directory Domain Services et DNS..."
Install-WindowsFeature -Name AD-Domain-Services, DNS -IncludeManagementTools
```

```
# Étape 3 : Configuration de la forêt et du domaine
Write-Host "Configuration de la forêt et du domaine..."
Install-ADDSForest `
   -DomainName $DomainName `
   -DomainNetBIOSName $NetBIOSName `
   -SafeModeAdministratorPassword $SafeModePassword ` #MDP Fort
   -Force `
   -InstallDNS `
   -DatabasePath "C:\NTDS" `
   -LogPath "C:\NTDS" `
   -SysvolPath "C:\SYSVOL" `
   -ForestMode $ForestMode `
   -DomainMode $ForestMode

Restart-Computer -Force

# Pause pour redémarrage
Start-Sleep -Seconds 60

# Étape 4 : Configuration de la redondance (ajout d'un deuxième contrôleur de domaine)
Write-Host "Ajout d'un deuxième contrôleur de domaine..."
$SecondDC = "DC02.mon-domaine.local"
Add-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Install-ADDSDomainController `
   -DomainName $DomainName `
   -InstallDNS `
   -Credential (Get-Credential) `
   -DatabasePath "C:\NTDS" `
   -LogPath "C:\NTDS" `
   -SysvolPath "C:\SYSVOL"
```

```
# Étape 5 : Vérification des FSMO

Write-Host "Vérification et répartition des rôles FSMO..."

Get-ADForest | Select-Object SchemaMaster, DomainNamingMaster

Get-ADDomain | Select-Object RIDMaster, PDCEmulator, InfrastructureMaster


# Étape 6 : Configuration des GPOs pour prescrire l'usage de périphériques amovibles

Write-Host "Configuration des GPOs..."

Import-Module GroupPolicy

$GPOBase = New-GPO -Name "Politique de base" -Domain $DomainName

Set-GPRegistryValue -Name "Politique de base" -Key
"HKLM\Software\Policies\Microsoft\Windows\RemovableStorageDevices" `

   -ValueName "Deny_All" -Type DWord -Value 1

New-GPLink -Name "Politique de base" -Target "DC=mon-domaine,DC=local"

# Résumé final

Write-Host "Déploiement terminé. Vérifiez chaque composant pour valider la configuration."


#Optionnel car il faut que chaque collaborateur ait une adresse mail définie sur le domaine de l'entreprise, cela ne fonctionnera donc pas dans la présente démonstration.

Write-Host "Mise en œuvre de l'authentification multifacteur (MFA)..."

Connect-MsolService

#Une fenêtre s'ouvre et nécessite l'authentification sur les services Microsoft, il peut être nécessaire de placer le lien dans une liste de confiance

$Mfa = New-Object -TypeName
Microsoft.Online.Administration.StrongAuthenticationRequirement

$Mfa.RelyingParty = "*"

$Mfa.State = "Enabled"

$MfaStatus = @($Mfa)

$Users = Get-ADGroupMember -Identity "O365-Licence-E3" | Foreach{ Get-ADUser -Identity
$_.SamAccountName } | Select-Object UserPrincipalName

$USers | Set-MsolUser -StrongAuthenticationRequirements $MfaStatus
```

8.2 Script déploiement Hyper-V + VM :

```
<#

.SYNOPSIS

Automatisation de l'installation et configuration d'Hyper-V sur Windows Server 2022.

.DESCRIPTION

Ce script installe le rôle Hyper-V, configure les commutateurs virtuels, et crée des machines virtuelles avec un disque virtuel.

.AUTHOR

Groupe 3

.LASTEDIT

02/12/2024

#>


# Étape 1 : Vérifier les pré-requis matériels pour Hyper-V

Write-Host "Vérification de la compatibilité matérielle pour Hyper-V..."

$HyperVSupport = Get-WindowsOptionalFeature -Online | Where-Object { $_.FeatureName -eq "Microsoft-Hyper-V" }

if ($HyperVSupport.State -ne "Enabled") {

   Write-Host "Hyper-V est compatible sur ce système. Procédons à l'installation." -ForegroundColor Green

} else {

   Write-Host "Hyper-V est déjà installé sur ce système." -ForegroundColor Yellow

   exit

}

# Étape 2 : Installation du rôle Hyper-V

Write-Host "Installation du rôle Hyper-V..."

Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart

# Pause pour redémarrage

Write-Host "Le serveur va redémarrer pour appliquer les modifications." -ForegroundColor Green

Start-Sleep -Seconds 60
```

```
# Étape 3 : Création d'un commutateur virtuel

Write-Host "Création d'un commutateur virtuel..."

$SwitchName = "SwitchVirtuel"

New-VMSwitch -Name $SwitchName -NetAdapterName "Ethernet" -AllowManagementOS $true


#Étape 4 : Création de la VM

# Définir les paramètres de la machine virtuelle

$VMName = "VM-Test"

$VMPath = "C:\Hyper-V\$VMName\"

$SwitchName = "SwitchVirtuel" # Nom du commutateur virtuel existant

$VMRAM = 4GB # Mémoire en octets (par exemple, 4 Go)

$VHDPath = "$VMPath$VMName.vhdx"

$VHDSizeBytes = 50GB # Taille du disque virtuel (en octets)

$ISOPath = "C:\Users\Administrateur\Downloads\ubuntu-24.04.1-live-server-amd64.iso"


# Créer le dossier pour la VM

if (!(Test-Path $VMPath)) { New-Item -ItemType Directory -Path $VMPath }


# Créer un disque virtuel

Write-Host "Création d'un disque virtuel pour la VM..."

New-VHD -Path $VHDPath -SizeBytes $VHDSize -Dynamic


# Créer la machine virtuelle

Write-Host "Création de la machine virtuelle '$VMName'..."

New-VM -Name $VMName `

-MemoryStartupBytes $VMRAM `

-Generation 2 `

-NewVHDPath $VHDPath `

-NewVHDSizeBytes $VHDSizeBytes `
```

```
# Configurer les processeurs
Write-Host "Configuration des processeurs pour la VM..."
Set-VMProcessor -VMName $VMName -Count 2

# Configurer le démarrage automatique
Write-Host "Activation du démarrage automatique pour la VM..."
Set-VM -Name $VMName -AutomaticStartAction StartIfRunning

# Étape 5 : Montage de l'ISO pour l'installation de l'OS
# Ajouter un lecteur DVD avec l'ISO
Write-Host "Ajout du lecteur DVD et montage de l'ISO..."
$CDDrive = Add-VMDvdDrive -VMName $VMName -Path $ISOPath

# Configurer le firmware pour démarrer sur le lecteur DVD
Write-Host "Configuration du firmware pour démarrer sur le DVD..."
Set-VMFirmware -VMName $VMName -FirstBootDevice $CDDrive

# Étape 6 : Démarrer la VM
Write-Host "Démarrage de la machine virtuelle..."
Start-VM -Name $VMName

# Étape 7 : Vérification de la configuration
Write-Host "Vérification de la configuration de l'environnement Hyper-V..."
Get-VM
Get-VMSwitch
Get-VMDisk -VMName $VMName

Write-Host "Configuration Hyper-V terminée avec succès !" -ForegroundColor Green
```

8.3 Script création d'un OU dynamique

```
<#
.SYNOPSIS
Création des OUs en masse à l'aide d'un fichier .csv à compléter en fonction de votre organigramme.
.DESCRIPTION
Ce script créer un OU avec l'ensemble des données nécessaires.
.AUTHOR
Groupe 3
.LASTEDIT
02/12/2024
#>
$CSVFile = "C:\OU.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8
$OUBase = "DC=mon-domaine,DC=local"

Foreach($OU in $CSVData) {
  $OUTitle = $OU.NomOU
  # Vérifier la présence de l'OU dans l'AD
  if (Get-ADOrganizationalUnit -Filter {Name -eq $GroupeTitle}) {
    Write-Warning "L'identifiant $GroupeTitle existe déjà dans l'AD"
  } else {
    # Création d'une OU
    New-ADOrganizationalUnit -Name $OUTitle `
                -Path $OUBase `
                -ProtectedFromAccidentalDeletion $true `
    Write-Output "OU créé : $OUTitle"
  }
}
```

8.4 Script création d'un groupe dynamique

```
<#

.SYNOPSIS

Création des groupes en masse à l'aide d'un fichier .csv à compléter en fonction de votre organigramme.

.DESCRIPTION

Ce script créer un groupe avec l'ensemble des données nécessaires, ainsi que sa localisation dans une OU.

.AUTHOR

Groupe 3

.LASTEDIT

02/12/2024

#>

$CSVFile = "C:\Groupe.csv"

$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8

$OUBase = "OU=Groupes,DC=mon-domaine,DC=local"


Foreach($Groupe in $CSVData) {
  $GroupeTitle = $Groupe.Groupe
  # Vérifier la présence du groupe dans l'AD
  if (Get-ADGroup -Filter {Name -eq $GroupeTitle}) {
    Write-Warning "L'identifiant $GroupeTitle existe déjà dans l'AD"
  } else {
    # Création d'un groupe
    New-ADGroup -Name $GroupeTitle `
          -GroupScope Global `
          -GroupCategory Security `
          -Path $OUBase `
    Write-Output "Groupe créé : $GroupeTitle"
  }
}
```

8.5 Script création d'utilisateur dynamique

```
<#

.SYNOPSIS

Création des utilisateurs en masse à l'aide d'un fichier .csv à compléter en fonction de votre organigramme.

.DESCRIPTION

Ce script créer un utilisateur avec l'ensemble des données nécessaires, ainsi que sa localisation dans une OU.

.AUTHOR

Groupe 3

.LASTEDIT

02/12/2024

#>

$CSVFile = "C:\Utilisateur.csv"

$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8

$OUBase = "OU=Utilisateurs,DC=mon-domaine,DC=local"


Foreach($Utilisateur in $CSVData) {

   $UtilisateurPrenom = $Utilisateur.Prenom

   $UtilisateurNom = $Utilisateur.Nom

   $UtilisateurLogin = ($UtilisateurPrenom).Substring(0,1) + "." + $UtilisateurNom

   $UtilisateurEmail = "$UtilisateurLogin@mon-domaine.local"

   $UtilisateurMotDePasse = "IT-Connect@2020"

   $UtilisateurFonction = $Utilisateur.Fonction

   $UtilisateurIdentity = $Utilisateur.Identity

   $UtilisateurGroupe = $Utilisateur.Fonction
```

```
    # Vérifier la présence de l'utilisateur dans l'AD
    if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin}) {
        Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
    } else {
        # Création de l'utilisateur
        New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
                -DisplayName "$UtilisateurNom $UtilisateurPrenom" `
                -GivenName $UtilisateurPrenom `
                -Surname $UtilisateurNom `
                -SamAccountName $UtilisateurLogin `
                -UserPrincipalName "$UtilisateurLogin@mon-domaine.local" `
                -EmailAddress $UtilisateurEmail `
                -Title $UtilisateurFonction `
                -Path $OUBase `
                -AccountPassword (ConvertTo-SecureString $UtilisateurMotDePasse -AsPlainText -
Force) `
                -ChangePasswordAtLogon $true `
                -Enabled $true

        Write-Output "Utilisateur créé : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"

        # Ajout de l'utilisateur au groupe
        try {
            Add-ADGroupMember -Identity $UtilisateurGroupe -Members $UtilisateurLogin
            Write-Output "Utilisateur $UtilisateurLogin ajouté au groupe $UtilisateurGroupe"
        } catch {
            Write-Error "Erreur lors de l'ajout de $UtilisateurLogin au groupe $GroupeCible : $_"
        }
    }
}
```

8.6 Script DHCP

```
# Installation du DHCP

Install-WindowsFeature -Name DHCP -IncludeManagementTools


# Importation des modules DHCP

Import-Module DHCPServer


# Définir les paramètres du pool DHCP

$ScopeName = "notrereseau"

$ScopeID = "192.168.1.0"

$SubnetMask = "255.255.255.0"

$StartIP = "192.168.1.100"

$EndIP = "192.168.1.200"

$DefaultGateway = "192.168.1.1"

$DNSServer = "192.168.1.2"


# Créer un nouveau pool DHCP

Add-DhcpServerv4Scope -Name $ScopeName -StartRange $StartIP -EndRange $EndIP -
SubnetMask $SubnetMask -State Active


# Configurer le DHCP (DNS/Gateway)

Set-DhcpServerv4OptionValue -ScopeId $ScopeID -DnsServer $DNSServer -Router
$DefaultGateway


# Activation du DHCP

Restart-Service -Name DhcpServer


Write-Host "Le serveur DHCP est configuré avec l'étendue '$ScopeName'."
```

Script permettant l'installation d'un DHCP avec les paramètres souhaités.