Gestion des strategies d execution et debloquage de scripts PowerShell

Etape 1 : Visualiser les stratégies d'exécution

1. Ouvrez PowerShell en mode administrateur.
2. Tapez la commande suivante pour afficher les stratégies d'exécution appliquees aux différents scopes : Get-ExecutionPolicy -List

```
PS C:\WINDOWS\system32> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser    RemoteSigned
 LocalMachine       Undefined
```

Etape 2 : Modifier la stratégie d'exécution utilisateur

1. Changez la stratégie d'exécution pour l'utilisateur courant afin d autoriser l'exécution des scripts locaux signes ou non :
2. Validez la modification en tapant T (Oui) lorsqu on vous le demande.

```
PS C:\WINDOWS\system32> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser
```

3. Verifiez que la modification est bien prise en compte avec : Get-ExecutionPolicy -List

```
        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser    RemoteSigned
 LocalMachine       Undefined
```

Etape 3 : Telechargement et debloquage d un script

1. Creez un fichier PowerShell appele MonScript.ps1 contenant la ligne suivante : Write-Host "Script PowerShell execute avec succes !"

```
PS C:\Users\calvi\Desktop> .\powershell.ps1
Script PowerShell execute avec succes !
```

2. Simulez un telechargement Internet en ajoutant la marque de blocage : - Sur ce fichier, faites un clic droit > Proprietes > cochez la case Debloquer > puis cliquez sur Appliquer.

3. Alternative : debloquez le fichier avec la commande PowerShell suivante : Unblock-File -Path "C:\\Chemin\\Vers\\MonScript.ps1"

```
PS C:\Users\calvi\Desktop> Unblock-File -Path "C:\Users\calvi\Desktop\powershell.ps1"
```

Etape 4 : Executer le script

1. Lancez l execution de votre script dans PowerShell avec : .\\MonScript.ps1
2. Observez le resultat et verifiez qu il s execute sans message d erreur.

```
PS C:\Users\calvi\Desktop> .\powershell.ps1
Script PowerShell execute avec succes !
```

Questions a rendre avec votre TP

1. Quelle est la politique d execution par defaut sur votre machine ?
Undefined

2. Pourquoi est-il necessaire de debloquer un script telecharge avant execution ?
Car il est bloqué par défaut

3. Quels sont les risques lies a l utilisation d une politique Bypass ?
L'Execution de script malveillant

4. Quelle politique d execution recommanderiez-vous en entreprise ? Pourquoi
RemoteSigned car elle est un bon compromis entre sécurité et fonctionnalité