Réalisation d'une maquette WEF & WEC

Jean-Marc Pouchoulon

octobre 2023

1 Mise en place d'une plateforme windows server 2019

Vous utiliserez les deux machines virtuelles créées lors du TP précédent.

2 Installation de Sysmon sur win-1 et win-2

Connectez-vous sur les deux machines virtuelles win-1 et win-2.

```
vagrant ssh win-1
vagrant ssh win-2
```

Utilisez le code powershell suivant pour installer Sysmon sur les deux machines virtuelles.

```
Invoke-WebRequest -Uri "https://download.sysinternals.com/files/Sysmon.zip" -OutFile
↪  "c:\users\vagrant\Desktop\Sysmon.zip"
Invoke-WebRequest -Uri
↪  "https://raw.githubusercontent.com/Neo23x0/sysmon-config/master/sysmonconfig-export-block.xml" -OutFile
↪  "c:\users\vagrant\Desktop\sysmonconfig-export-block.xml"
Expand-Archive -F c:\users\vagrant\desktop\Sysmon.zip -DestinationPath c:\users\vagrant\desktop\sysmon
# version amélioré de switf on security
c:\users\vagrant\desktop\sysmon\sysmon64.exe -accepteula -i c:\users\vagrant\desktop\sysmonconfig-export-block.xml
```

Vérifiez que Sysmon alimente bien le journal des événements de Windows et son channel Microsoft-Windows-Sysmon/Operational.

Sauvegarder les logs Sysmon dans un fichier evtx à l'aide wevtutil.exe.

```
wevtutil query-events /c:5  Microsoft-Windows-Sysmon/Operational
wevtutil export-log Microsoft-Windows-Sysmon/Operational sysmon.evtx
wevtutil export-log WecFwdLog-Domain-Members/Security  security-apt.evtx
wevtutil export-log WecFwdLog-Domain-Members/Sysmon  sysmon-apt.evtx
```

3 Installation de WEC sur win-1

Utilisez la procédure d'installation d'un serveur WEC en image ici. La machine win-1 sera le serveur WEC. win-2 initiera les abonnements aux journaux d'événements de win-1 ("source computer initiated") sur le channel "forwarded events". C'est le système de fonctionnement plébiscité par les experts Microsoft. Les clients WEC seront configurés par GPO. Chaque nouveau PC ajouté au domaine "forwardera" automatiquement des logs sur le serveur WEC (win-1).

4 Deploiement de la GPO WEF sur win-2

Construisez ensuite une GPO pour déployer la configuration WEF sur win-2 en suivant la procédure suivante ici