GPO Sysmon Install

GPO ile Sysmon Kurulumu Adımları

1. **Sysmon'un İndirilmesi:**
   İlk olarak, Sysmon'un resmi Microsoft Teknik Destek web sitesinden indirilmesi gerekmektedir. Sysmon'un en son sürümünü
   Microsoft Sysinternals web sitesinden indirebilirsiniz.
2. **Sysmon Konfigürasyon Dosyasının Hazırlanması:**
   Sysmon'u dağıtmak için bir konfigürasyon dosyası (XML formatında) oluşturmanız gerekmektedir. Bu konfigürasyon dosyası, Sysmon'un hangi olayları izleyeceğini ve nasıl davranacağını tanımlar. Örneğin, aşağıdaki gibi bir XML dosyası kullanılabilir:

```
<Sysmon schemaversion="4.50">
    <EventFiltering>
        <RuleGroup name="ProcessCreate" groupRelation="o
r">
            <ImageLoad onmatch="include">
                <Image condition="is">*</Image>
            </ImageLoad>
        </RuleGroup>
        <RuleGroup name="NetworkConnect" groupRelation="o
r">
            <NetworkConnect onmatch="include">
                <DestinationPort condition="is">80</Destin
ationPort>
            </NetworkConnect>
        </RuleGroup>
        <!-- Diğer kurallar buraya eklenebilir -->
    </EventFiltering>
</Sysmon>
```

Bu örnek XML dosyası, tüm işlemleri ve 80 numaralı bağlantı noktasına yapılan ağ bağlantılarını izler.

Kapsamlı ve tavsiye edilen XML dosyası örneği https://github.com/SwiftOnSecurity/sysmon-config/tree/master adresinde bulunmaktadır.

3. **GPO Hazırlığı:**
   Sysmon'u dağıtmak için bir GPO oluşturmanız gerekmektedir.
   - **Yeni bir GPO Oluşturma:**
     1. **Group Policy Management Console (GPMC)** açın.
     2. Gerekli Organizational Unit (OU) üzerinde sağ tıklayın ve "Create a GPO in this domain, and Link it here" seçeneğini seçin.
     3. GPO'ya bir ad verin (örneğin, "Sysmon Deployment").
   - **GPO Ayarlarının Yapılandırılması:**
     1. Oluşturulan GPO'yu seçin, sağ tıklayın ve "Edit" seçeneğini seçin.
     2. GPO Yönetim Editörü açılacak. Buradan `Computer Configuration -> Policies -> Software Settings -> Software Installation` altına gelin.
     3. Sağ tıklayarak "New → Package" seçeneğini seçin ve indirdiğiniz Sysmon MSI dosyasını seçin.
4. **Sysmon Konfigürasyon Dosyasının Dağıtılması:**
   Sysmon kurulumunu yapılandırdıktan sonra, Sysmon'u dağıtmak için GPO'ya bir logon script veya PowerShell scripti ekleyebilirsiniz. Bu script, Sysmon konfigürasyon dosyasını hedef makinelerin `C:\\Windows` dizinine kopyalayabilir ve ardından Sysmon'u yapılandırabilir.

   Örneğin, PowerShell kullanarak Sysmon'u dağıtmak için aşağıdaki gibi bir script kullanabilirsiniz:

```
# Sysmon dosyalarını kopyala
Copy-Item -Path "\\\\fileserver\\sysmon\\sysmon.exe" -Dest
ination "C:\\Windows\\" -Force
Copy-Item -Path "\\\\fileserver\\sysmon\\sysmonconfig.xml"
-Destination "C:\\Windows\\" -Force
```

```
# Sysmon'u yapılandır
Start-Process -FilePath "C:\\Windows\\sysmon.exe" -Argumen
tList "/accepteula -i C:\\Windows\\sysmonconfig.xml"
```

Bu PowerShell scriptini, GPO ile "Logon" script olarak ayarlayabilir veya uzaktan oturum açma işlemi için bir yönetici olarak çalıştırarak Sysmon'u dağıtabilirsiniz.

5. **GPO'nun Uygulanması:**
   - GPO'yu doğru Organizational Unit (OU) veya domain seviyesinde ilgili bilgisayarlar için uygulayın.
   - GPO'nun etkin olması için hedef bilgisayarların yeniden başlatılmasını bekleyin veya `gpupdate /force` komutunu çalıştırarak GPO'nun hemen uygulanmasını sağlayabilirsiniz.

EN

Deploying Sysmon via Group Policy Objects (GPO) is a straightforward process for managing Windows-based computers within an Active Directory environment. Sysmon (System Monitor) is a robust system monitoring tool for Windows OS commonly used for security event monitoring. Here are the step-by-step instructions for deploying Sysmon using GPO:

Steps to Deploy Sysmon via GPO

1. **Download Sysmon:**
   First, download the latest version of Sysmon from the official Microsoft Sysinternals
   website.
2. **Prepare Sysmon Configuration File:**
   To deploy Sysmon, you need to create a configuration file in XML format that defines what events Sysmon will monitor and how it will behave. For example, here is a sample XML configuration:

```
<Sysmon schemaversion="4.50">
    <EventFiltering>
```

```
        <RuleGroup name="ProcessCreate" groupRelation="o
r">
            <ImageLoad onmatch="include">
                <Image condition="is">*</Image>
            </ImageLoad>
        </RuleGroup>
        <RuleGroup name="NetworkConnect" groupRelation="o
r">
            <NetworkConnect onmatch="include">
                <DestinationPort condition="is">80</Destin
ationPort>
            </NetworkConnect>
        </RuleGroup>
        <!-- Add other rules here -->
    </EventFiltering>
</Sysmon>
```

This example XML file monitors all process creations (`ProcessCreate`) and network connections to port 80 (`NetworkConnect`).

3. **Prepare the Group Policy Object (GPO):**
   - **Create a New GPO:**
     1. Open the Group Policy Management Console (GPMC).
     2. Right-click on the necessary Organizational Unit (OU) and select "Create a GPO in this domain, and Link it here".
     3. Give the GPO a name (e.g., "Sysmon Deployment").
   - **Configure GPO Settings:**
     1. Select the newly created GPO, right-click, and choose "Edit".
     2. The Group Policy Management Editor will open. Navigate to `Computer Configuration -> Policies -> Software Settings -> Software Installation`.
     3. Right-click, select "New → Package", and choose the Sysmon MSI file you downloaded.

4. **Distribute the Sysmon Configuration File:**
   After configuring Sysmon installation, you can distribute the Sysmon configuration file to target machines using a logon script or PowerShell script via GPO. This script can copy the Sysmon configuration file to the `C:\\Windows` directory on target machines and then configure Sysmon.

   For example, you can use the following PowerShell script to deploy Sysmon:

   ```
   # Copy Sysmon files
   Copy-Item -Path "\\\\fileserver\\sysmon\\sysmon.exe" -Dest
   ination "C:\\Windows\\" -Force
   Copy-Item -Path "\\\\fileserver\\sysmon\\sysmonconfig.xml"
   -Destination "C:\\Windows\\" -Force

   # Configure Sysmon
   Start-Process -FilePath "C:\\Windows\\sysmon.exe" -Argumen
   tList "/accepteula -i C:\\Windows\\sysmonconfig.xml"
   ```

   You can set this PowerShell script as a "Logon" script in the GPO or run it as an administrator for remote session to deploy Sysmon.

5. **Apply the GPO:**
   - Apply the GPO to the appropriate Organizational Unit (OU) or at the domain level for relevant computers.
   - Ensure the GPO is applied by restarting the target computers or running `gpupdate /force` command to enforce immediate GPO application.

These steps provide a guideline for deploying and configuring Sysmon via GPO tailored to your system and network security requirements.