

# Konfigürasyon

Sysmon, kurulduğunda kendi konfigürasyon ayarlarına göre kurulum yapar fakat kullanıcılar bu konfigürasyon ayarlarını kendilerine göre düzenleyebilir. Sysmon, konfigürasyon dosyalarını xml biçiminde depolar.

```
<Sysmon schemaversion="3.30">
  <HashAlgorithms>md5,sha256</HashAlgorithms>
  <EventFiltering>

  </EventFiltering>
</Sysmon>
```

Konfigürasyon dosyası için 2 ana bölüm bulunmaktadır.

HashAlgorithms, bölümünde oluşturulan processlerin hangi hash algoritmalarını kullanılacağını belirtmek için kullanılır.

EventFiltering, özellikle izlenen veya hariç tutulan olayları belirtmek için kullanılır.

Include, olayları dahil etmek için kullanılır. Exclude, olayları hariç tutmak için kullanılır.

```
<tag onmatch="include">
  ...
  ...
</tag>
```

```
<tag onmatch="exclude">
  ...
  ...
</tag>
```

Filtrelemede kullanılan tagların listesi aşağıdaki gibi sıralanmıştır.

<b>ProccesCreate</b>	Süreç Oluşturur
<b>ProccesTerminate</b>	İşlem sonlandırır
<b>FileCreateTime</b>	Dosya oluşturma zamanı
<b>NetworkConnect</b>	Ağ bağlantısı kontrolü

<b>DriverLoad</b>	Sürücü yükleme kontrolü
<b>ImageLoad</b>	Resim yükleme kontrolü
<b>CreateRemoteThread</b>	Uzak Konu Oluştur
<b>RawAccessRead</b>	Ham Erişim Okuması

Condition tipleri ve özellikleri:

<b>is</b>	Varsayılan, değerler eşittir
<b>is not</b>	Farklı değerler
<b>contains</b>	Alan bu değeri içeriyor
<b>excludes</b>	Alan bu değeri içermiyor
<b>begin with</b>	Alan bu değerle başlar
<b>end with</b>	Alan bu değerle biter
<b>less than</b>	Sözlükbilimsel karşılaştırma sıfırdan küçüktür
<b>more than</b>	Sözlükbilimsel karşılaştırma sıfırdan büyüktür
<b>image</b>	Bir resim yolunu eşleştirin (tam yol veya yalnızca resim adı)

Revision #1  
Created 27 January 2024 15:58:40 by Ertan Sözer  
Updated 27 January 2024 16:00:34 by Ertan Sözer