Konfigürasyon

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

Konfigürasyon dosyası için 2 ana bölüm bulunmaktadır.

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

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

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

Filtrelemede kullanılan tagların listesi aşağıdaki gibi sıralanmıştır.

ProccesCreate	Süreç Oluşturur
ProccesTerminate	İşlem sonlandırır
FileCreateTime	Dosya oluşturma zamanı
NetworkConnect	Ağ bağlantısı kontrolü

DriverLoad	Sürücü yükleme kontrolü
İmageLoad	Resim yükleme kontrolü
CreateRemoteThread	Uzak Konu Oluştur
RawAccessRead	Ham Erişim Okuması

Condition tipleri ve özellikleri:

is	Varsayılan, değerler eşittir
is not	Farklı değerler
contains	Alan bu değeri içeriyor
excludes	Alan bu değeri içermiyor
begin with	Alan bu değerle başlar
end with	Alan bu değerle biter
less than	Sözlükbilimsel karşılaştırma sıfırdan küçüktür
more than	Sözlükbilimsel karşılaştırma sıfırdan büyüktür
image	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