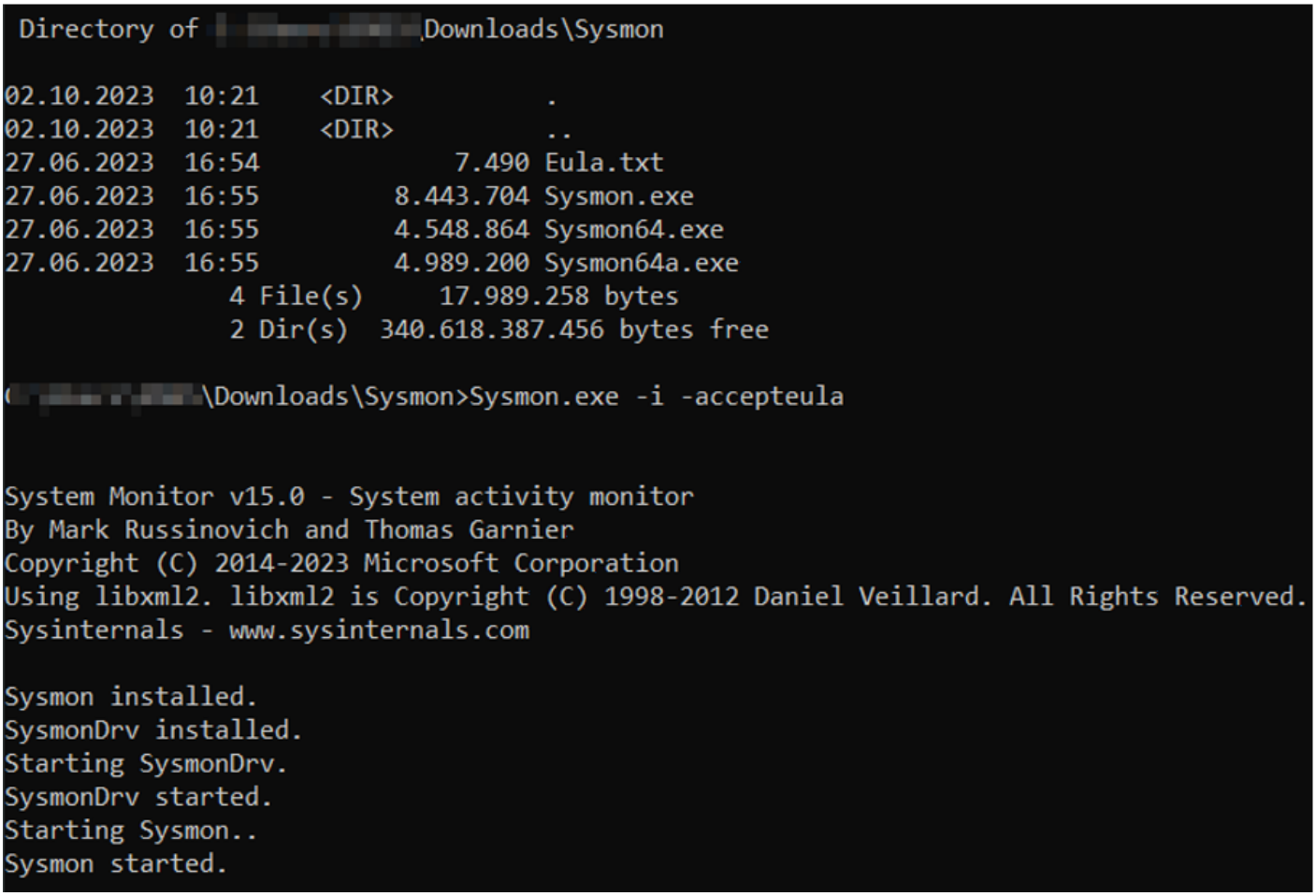
Kurulum

Kurulum

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon adresinden sysmon indirilir.

Cmd ile indirilen dosya konumuna gidilir ardından Sysmon'u default ayarlarda çalıştırmak için "Sysmon.exe –i –accepteula" komutu girilir.



Sysmon kullanımına ait detayları görmek için Sysmon –h komutu kullanılır.

```
[redacted]\Downloads\Sysmon>sysmon -h


System Monitor v15.0 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install:                Sysmon.exe -i [<configfile>]
Update configuration:   Sysmon.exe -c [<configfile>]
Install event manifest: Sysmon.exe -m
Print schema:           Sysmon.exe -s
Uninstall:              Sysmon.exe -u [force]
  -c   Update configuration of an installed Sysmon driver or dump the
       current configuration if no other argument is provided. Optionally
       take a configuration file.
  -i   Install service and driver. Optionally take a configuration file.
  -m   Install the event manifest (done on service install as well)).
  -s   Print configuration schema definition of the specified version.
       Specify 'all' to dump all schema versions (default is latest)).
  -u   Uninstall service and driver. Adding force causes uninstall to proceed
       even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity
from early in the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services
Logs/Microsoft/Windows/Sysmon/Operational". On older systems, events are written to the System event
log.

Use the '-? config' command for configuration file documentation. More examples are available on the
Sysinternals website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be
interactively prompted to accept it.

Neither install nor uninstall requires a reboot.
```

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 izlenilen veya hariç tutulan olayları belirtmek için kullanılır.

İnclude, 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.

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)