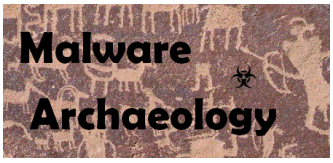
WINDOWS SYSMON LOGGING CHEAT SHEET – up to ver 10.2

This "**Windows Sysmon Logging Cheat Sheet**" is intended to help you understand where Microsoft's FREE Sysinternals Sysmon agent can supplement and enhance your Windows Logging, NOT replace it. Sysmon can provide more information than standard default Windows logs provide. Sysmon is great to collect data you need for Incident Response, malware labs, high security situations, your own personal systems, or just improve the existing log data you are collecting with more details.



LOG-MD
Discover it

OVERVIEW:

What is it?: Sysmon is a shttps:ervice that you add to a Windows system. For the purposes of this Cheat Sheet, only the items that supplement or enhance existing Windows logging will be covered. The intention of this Cheat Sheet is also to understand it is NEVER recommended to use Sysmon instead of the built-in Windows audit logging as Sysmon can be easily turned off, bypassed, or corrupted (see talk by Carlos Perez under Resources). Use the various Windows Logging Cheat Sheets first, then supplement them with Sysmon. For the latest on Sysmon, please visit the main Sysinternals Sysmon page:

- https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

IMPORTANT NOTE: Sysmon is a FREE and ***unsupported*** utility, meaning you cannot get, or pay for support. You can visit the community page and post an issue, or use Twitter, but for production environments you are on your own, so thoroughly test it and use it at your own risk.

COLLECTION INTO LOG MANAGEMENT SOLUTIONS:

Sysmon is VERY noisy when it comes to generating events, more so than standard Windows logs even with all of the Cheat Sheets fully enabled. When collecting Sysmon events into log management, be sure to utilize the config.xml to "include" and/ or "exclude" what you collect with Sysmon and to "collect only the right things", or "reduce as many things as you know are normal". You may also be able to use your log collection agent (WinLogBeat, NxLog, Splunk Universal Forwarder, etc.) to reduce or limit what you actually collect into log management. You can see examples of these log agent configurations at:

- https://www.malwarearchaeology.com/logging

You can still collect more in the local Sysmon log that you can investigate and/or harvest if needed with say, a tool like LOG-MD-Professional that can harvest most Sysmon events.

LOG SIZE:

A VERY important detail to Sysmon is the size of the "***Applications and Services Logs - Microsoft-Windows-Sysmon/Operational***" log. The default log size will not collect much of anything as the data will roll in minutes or faster depending on what you collect. You can use LOG-MD Free or LOG-MD Professional to audit the current log size. It is HIGHLY recommended that the ***Sysmon/Operational*** log be set to:

- 1,024,000GB
  - WevtUtil sl Security /ms: 1048576000 or /ms: 2097152000 for Servers or if you decide to collect all the things – Set the Microsoft-Windows-Sysmon/Operational Security log size to the number of bytes
- Set manually in EventViewer to 1,024,000 or 2,048,000

Check the log size with the following command or use LOG-MD -a:

- WevtUtil gl Microsoft-Windows-Sysmon/Operational

OVERVIEW:

AV and EDR:

It is important to note that many Anti-Virus and EDR solutions should have the Sysmon binary and driver excluded from being scanned or performance impacts may be overwhelming.

Service, Registry and File monitoring: It is strongly recommended that if you are going to use Sysmon in production that you monitor changes to the Sysmon Registry keys and config.xml file (or whatever you end up naming and placing it) to monitor for any attacks and/or changes against the service. Sysmon will not register an event if the key values are changed, so built-in Windows auditing (Security log Event ID 4657) can be used. Follow the '***Windows Registry Auditing Cheat Sheet***' for more on auditing registry keys. Windows will NOT register a Service STOP or START for Sysmon (System log Event ID 7040), you will need to follow the '***Windows Advanced Logging Cheat Sheet***' to set the DACLs on the Sysmon service to trigger an event. Sysmon ID 4 in the Sysmon/Operational log will register the service has been stopped, if it has not rolled or been cleared, or messed with. You could also look for Security log Event IDs 4688 (Process Started), and 4689 (Process Terminated) to watch for Sysmon process behavior. The following Registry Keys and files should be monitored:

- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sysmon64
- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysmonDrv
- The config.xml file that you named and where it is placed.

Config.xml: The default name for the Sysmon config.xml of course should be changed and moved so that is not in the obvious default location of C:\Windows. Keep in mind that by reading your config.xml file, an attacker can know just by reading this file what you are, or are not recording with Sysmon. You may want to craft an auditing rule to monitor reads to this file by something other than Sysmon and filter out your security tools that may read this file normally.

Also keep in mind that this config file can get very large the more you collect and exclude and/or include. Large config files are also going to be harder to manage and easier to mess with from an attackers perspective. It is recommended to keep config files small and refined, collect only what you REALLY need, versus all the things.

Tuning Sysmon: One of the more cumbersome tasks of Sysmon will be to tune the config.xml file that you use and create to include what you want, and/or exclude what you do not want to collect.

Malware Archaeology takes a MUCH different approach to using Sysmon than many of the resources listed at the Resources section below. It was already stated that Sysmon should be used to "supplement" already existing Windows logging, so consider what you should collect, taking into account includes and excludes in the config.xml file. Consider the quantity of events Sysmon will collect, versus what you already collect with the Windows logging with all the other cheat sheets.

Includes vs Excludes: You either have to select to include something and/or exclude items in the config.xml. Includes provide the ability to TAG items as they are logged giving you something to search on in a log management console such as a MITRE ATT&CK Technique ID. Excludes drop things from being logged so you collect less items.

Recommendation: Use EXCLUDES over includes.

OVERVIEW:

Includes vs Excludes: continued

Of course there are cases that make sense that you would use include and exclude statements in your config.xml. Items that you want to collect that are noisy and generate a LOT of events, you might only include specific locations for some selected items. For example: It is recommended to monitor the '***C:\Users***' directory structure for new files. If you want to monitor for file writes and exclude all the normal items, this could be overly noisy. So you might only include certain directories, versus excluding all the normal writes/creates. The problem with includes is that it must exist to be included, so how does one include a new directory(s) malware might create?

Also by reading a config.xml that has includes, an attacker would know where you are monitoring and exploit some place you are not. An exclude could also be misused by using a location that is excluded from being monitored. So give what you are including versus excluding some serious thought and overlap what you exclude with one Event ID with another. It is recommended to filter out what you know is normal and avoid, or use includes sparingly. I am sure this statement will stir some debate, but remember the goal is to look for "unknown unknowns" and includes generally cannot do this function. Of course there are always good uses for includes, in the end it is up to you to decide.

DIFFERENT USES of the config.xml:

- **Malware Labs** – Generally collecting all the things is OK and recommended in this use case and only exclude normal baseline image items. The more information collected the better.
- **Your personal and work systems** – A great use of excludes only and limit what you collect as to not generate a ton of events for log management, This is a good place to practice using a tuned Sysmon config.xml and a combination of your log management endpoint agent configuration.
    - Consider using a FREE solution like Humio or other log management solution to collect your system logs, see what you are collecting, what could be tweaked, and reduced to optimize your config.xml as well as your endpoint agent configuration of what you send to log management. There is a "***Humio Logging Cheat Sheet***" to help you get started with this, along with all the other Cheat Sheets of course.
- **Incident Response** – This may be similar to a malware lab in that you have a base config.xml that you push out to a system that you are investigating, or is high risk that you want to monitor. Pay attention to how far back the local logs store data and falls off the log. Adjust the log size accordingly.
- **Production systems** – Use Sysmon with excludes of normal baseline items for that system to generate as little as possible and collect only very actionable high value items. Consider CPU, memory and total events generated before rolling out into production, and use Group Policy to control configurations as much as possible.
- **High Risk systems** – Use Sysmon to monitor systems that pose a high risk, either to lack of, or inability to patch, exposed to the Internet, cannot be fully locked down, etc. A combination of excludes and includes might be used in this example.

WHAT TO COLLECT?:

Sysmon Event IDs of high value:

There are now 23 Sysmon Event IDs. They collect all kinds of things that also duplicate what Windows natively collects or adds something that Windows does not create, like the hash of an executing process, or a GUID to track related items. The trick to "collecting the right things" and not get event overwhelmed will be your challenge with Sysmon. The table below will provide a recommended starting configuration to "collect the right things" with not being overly noisy. All recommendations will be for Windows 10 or Server 2016 and later as there are more items collected with newer versions of Windows.

Sysmon Config.xml recommendations compared to Windows logs

This is an example to help understand where the overlap between Windows logs and what Sysmon covers.

Sysmon ID	Windows ID(s)	Event Type	Note	Valuable Additional Data	Production Recommendation	Malware Lab
1	Security - 4688	Process Creation	Noisy (3)	Hash of the process/file	Use Windows	Use both
2	Security - 4657	Process Changed a file creation time			Use Windows	Use both
3	Security - 5156	Network Connection	Noisy (3)	Provides some name resolution of IP	Use Windows	Use both
4	(1)	Sysmon Service State Change			Collect	Use both
5	Security - 4689	Process Terminated	Noisy (3)		Use Windows	Use both
6	System 6, 219, 7026	Driver Loaded			Collect	Use both
7	n/a	Image Loaded	Noisy (3)	Most malware is NOT Signed, so is .NET	Collect Signed False only	Use both
8	n/a	Create Remote Thread			Optional	Use both
9	n/a	Raw File Access Read			Optional	Use both
10		Process Access	Noisy (3)		Optional	Use both
11	4663	File Create	Noisy (3)		Include only (2)	Use both
12	4657	Registry Create and Delete	Noisy (3)		Include only (2)	Use both
13	4657	Registry Value Set	Noisy (3)		Include only (2)	Use both
14	4657	Registry Key and Value Rename			Collect	Use both
15	n/a	File Create Stream Hash			Collect	Use both
16	(1)	Sysmon Config Change			Collect	Use both
17	n/a	Pipe Event Created			Collect	Use both
18	n/a	Pipe Event Connected			Collect	Use both
19	5861, 5858, 5859	WMI EventFilter activity			Use Windows (4)	Use both
20	5861, 5858, 5859	WMI EventConsumer activity			Use Windows (4)	Use both
21	5861, 5858, 5859	WMI EventConsumerToFilter activity			Use Windows (4)	Use both
22	1016, 3008, 3010, 3020	DNS Query	Noisy (3)	Process that made the DNS Query	Use Windows (4)	Use both
255	n/a	Sysmon error			Collect	Use both
LEGEND						
All	Sysmon provides a ProcessGUID that allows you to link all events to a process - Benefit for tracking related events					
(1)	Refer to the Windows Advanced Logging Cheat Sheet on how to monitor Service with built-in Windows logging					
(2)	It is recommended to use Windows logging as the primary source, enable a policy of what you want to audit and apply to all systems					
(3)	These events are incredibly noisy and will effect how long you can keep a history in the local logs - These will take a lot of time to filter down					
(4)	Sysmon is optional, but pick only one					

For Incident Response situations, you might have a refined configuration that you use that is more than Production, but less than a Malware Lab.

Filtering Sysmon Events

You can access help from Sysmon with "***Sysmon -h***" or "***Sysmon64 -h***" depending which version you installed. You can also get detailed information from running the Sysmon config help using:

- Sysmon /? config

EVENT FILTERING CONDITIONS:

1. FILTERING OUT SYSMON EVENTS: You can use a configuration file to filter out log data that is not important or you deem noisy. Reducing events also has the benefit of reducing log size and if sending logs to a log management solution, reduce the logs you will collect helping to reducing licensing and storage requirements.
2. Do not be overly broad with exclusions. You want to be very specific on exclusions as much as possible. For example exclude by the full path and binary versus just excluding a whole folder. Excluding a whole folder means the bad guys can place or execute things in that folder and you may not get alerted. Being specific with exclusions is a good thing. It will however mean more rules will be needed to exclude each item, so use broad exclusions sparingly.
3. Keep config files organized. Keep similar type items together, folders, image, contains, etc. This will make it easier to maintain and find things as you maintain your configs. Use comments!
4. Consider ignoring Browsers on endpoints. This accounts for a TON of events. It's what happens outside the browser that is usually more important. You can always enable collection during an incident.

Conditions are case insensitive

Condition	Description
is	**Default, values are equals**
is not	**Values are different**
contains	**The field contains this value**
excludes	**The field does not contain this value**
begin with	**The field begins with this value**
end with	**The field ends with this value**
less than	**Lexicographical comparison is less than zero**
more than	**Lexicographical comparison is more than zero**
image	**Match an image path (full path or only image name). For example: lsass.exe will match c:\windows\system32\lsass.exe**

Sample Config.xml file

This is by no means an extensive list, this is a sample of the types of inclusions and exclusions you can do. This example is mostly for a production system, not a malware lab.

Config.xml sample:

1. FILTERING OUT SYSMON EVENTS: You can use a configuration file to filter out log data that is not important or you deem noisy. Reducing events also has the benefit of reducing log size and if sending logs to a log management solution, reduce the logs you will collect helping to reducing licensing and storage requirements.

```
<Sysmon schemaversion="4.21">
                <HashAlgorithms>SHA256</HashAlgorithms>

        <EventFiltering>

<!--Event ID 1 Process created -->
        <ProcessCreate onmatch="include">
                <Image name="Id='T1234',Tech='Blue Team WINS'" condition="contains">LOG-MD-Pro.exe</Image>
        </ProcessCreate>

<!--Event ID 1 Process created -->
        <ProcessCreate onmatch="exclude">
        <!—Program Files x86 -->
                <Image condition="image">C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</Image>
                <Image condition="image">C:\Program Files (x86)\Google\Update\GoogleUpdate.exe</Image>
                <Image condition="contains">C:\Program Files (x86)\Google\Update</Image>
                <Image condition="image">C:\Program Files (x86)\Notepad++\notepad++.exe</Image>
                <Image condition="image">C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe</Image>
        <!—Windows System32 -->
                <Image condition="image">C:\Windows\System32\SearchFilterHost.exe</Image>
                <Image condition="image">C:\Windows\System32\SearchProtocolHost.exe</Image>
                <Image condition="image">C:\Windows\System32\audiodg.exe</Image>
        </ProcessCreate>

<!--Event ID 2 Process changed Created Time -->
        <FileCreateTime onmatch="exclude">
                </FileCreateTime>

<!--Event ID 3 Network Connections -->
        <NetworkConnect onmatch="exclude">
                <DestinationHostname condition="contains">akamaitechnologies.com</DestinationHostname>
                <DestinationIp condition="contains">808:808:</DestinationIp>
                <DestinationIp condition="contains">fe80:0:0</DestinationIp>
                <DestinationIp condition="contains">ff02:0</DestinationIp>
                <DestinationIp condition="contains">e000:fc</DestinationIp>
                <DestinationIp condition="contains">a96:7849:</DestinationIp>
                <DestinationIp condition="contains">aa0:7855:</DestinationIp>
                <DestinationIp condition="contains">239.255.255.250</DestinationIp>
                <DestinationIp condition="contains">224.0.0.251</DestinationIp>
                <DestinationIp condition="contains">255.255.255.255</DestinationIp>
                <SourceIp condition="contains">224.0.0.25</SourceIp>
                <SourceIp condition="contains"> 239.255.255.250</SourceIp>
        </NetworkConnect>
```

Config.xml sample: continued

```
<!--Event ID 5 Process Terminated -->
        <ProcessTerminate onmatch="exclude">
                <Image condition="image">C:\Windows\System32\backgroundTaskHost.exe</Image>
                <Image condition="image">C:\Windows\System32\taskhostw.exe</Image>
                <Image condition="image">C:\Windows\System32\Speech_OneCore\common\SpeechRuntime.exe</Image>
        </ProcessTerminate>

<!--Event ID 6 Driver Load -->
        <DriverLoad onmatch="exclude">
                </DriverLoad>

<!--Event ID 7 ImageLoad -->
        <ImageLoad onmatch="exclude">
        <!—Only collect False signed modules -->
                <Signed condition="image">true</Signed>
        <!—Program Files x86 -->
                <Image condition="image">C:\Program Files (x86)\WinMerge\ShellExtensionX64.dll</Image>
                <Image condition="image">C:\Program Files\7-Zip\7-zip.dll</Image>
                <Image condition="image">C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</Image>
                <Image condition="contains">C:\Program Files (x86)\Google\Update</Image>
        <!—Windows System32 -->
                <Image condition="image">C:\Windows\System32\SearchFilterHost.exe</Image>
                <Image condition="image">C:\Windows\System32\SearchProtocolHost.exe</Image>
                <Image condition="image">C:\Windows\System32\audiodg.exe</Image>
        <!—Contains -->
                <Image condition="contains">LOG-MD-Pro.exe</Image>
        </ImageLoad>

<!--Event ID 8 CreateRemoteThread -->
        <CreateRemoteThread onmatch="exclude">
                </CreateRemoteThread>

<!--Event ID 9 RawAccessRead -->
        <RawAccessRead onmatch="exclude">
                <Image condition="image">System</Image>
                <Image condition="contains">C:\Windows\SystemApps\Microsoft.Windows.Cortana</Image>
                <Image condition="image">C:\Windows\System32\svchost.exe</Image>
                <Image condition="image">C:\Windows\System32\CompatTelRunner.exe</Image>
                <Image condition="image">C:\Windows\System32\SearchIndexer.exe</Image>
        </RawAccessRead>

<!--Event ID 10 ProcessAccess -->
        <ProcessAccess onmatch="include">
                </ProcessAccesS>
```

Config.xml sample: continued

```
<!--Event ID 11 FileCreate -->
        <FileCreate onmatch="exclude">
                <Image condition="image">C:\Program Files (x86)\Notepad++\notepad++.exe</Image>
                <Image condition="image">C:\Program Files (x86)\Mozilla Firefox\firefox.exe</Image>
                <Image condition="image">C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</Image>
                <Image condition="contains">C:\Users\BOB\AppData\Local\Microsoft\OneDrive</Image>
                <Image condition="contains">C:\WINDOWS\SystemApps\Microsoft.Windows.Cortana_</Image>
        <!—Target Filename -->
                <TargetFilename condition="image">C:\Program Files\WindowsApps\Microsoft.YourPhone</TargetFilename>
                <TargetFilename condition="image">C:\Program Files\WindowsApps\Microsoft.Microsoft3DViewer</TargetFilename>
                <TargetFilename condition="image">C:\ProgramData\Microsoft\Windows\AppRepository\Packages</TargetFilename>
        </FileCreate>

<!--Event ID 12, 13, 14 Registry Events -->
        <RegistryEvent onmatch="exclude">
                </RegistryEvent>

<!--Event ID 15 File Create Stream and Hash -->
        <FileCreateStreamHash onmatch="exclude">
                </FileCreateStreamHash>

<!--Event ID 17 and 18 Pipe Event -->
        <PipeEvent onmatch="exclude">
                <Image condition="image">C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</Image>
        </PipeEvent>

<!--Event ID 19,20,21 - WMI Events -->
        <WmiEvent onmatch="exclude">
                </WmiEvent>

<!--Event ID 22 - DNS Events -->
        <DnsQuery onmatch="exclude">
                <QueryName condition="contains">microsoft.com</QueryName>
        </DnsQuery>

        </EventFiltering>
</Sysmon>
```

RESOURCES:

1. Sysinternals website: https://technet.microsoft.com/en-us/sysinternals
    a. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
2. jymcheong/SysmonResources - https://github.com/jymcheong/SysmonResources
3. Google! – But of course

VAST LIST OF SYSMON RESOURCE:

1. Sysmon – DFIR
    a. https://github.com/MHaggis/sysmon-dfir

ATTACKING SYSMON:

1. Carlos Perez talk at DakotaCon 2018 - https://www.youtube.com/watch?v=ED1PaCypnek&feature=youtu.be&t=6h7m27s